AUSA Matthew Roth 313-226-9186
Special Agent Eric Clark 313-226-1825

WI (15)

AO 91 (Rev. 08/09) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Eastern District of Michigan

United States of America
v.
Matthew T. Creely

Case:2:12-mj-30562
Judge: Unassigned,
Filed: 09-12-2012 At 02:24 PM
CMP USA V. MATTHEW CREELY (WI)(AC)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of 6/6/12 and 6/7/12 in the county of Wayne in the Eastern District of Michigan, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. 2252A(a)(2) and (a)(5)(B)	Distribution, receipt and possession of child pornography.

This criminal complaint is based on these facts:

See attached Affidavit

☑ Continued on the attached sheet.

Complainant's signature

Eric S. Clark, Special Agent U.S. Secret Service
Printed name and title

Sworn to before me and signed in my presence.

Date: September 12, 2012

Judge's signature

City and state: Detroit, MI

David R. Grand, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT

I, Eric Clark, being first duly sworn, hereby depose and say:

1. I am a Special Agent with the United States Secret Service (USSS) assigned to the Detroit Field Office. I have been employed in this capacity since May 2004. I am currently assigned to the Michigan Internet Crimes Against Children (ICAC) task force. The Michigan ICAC is a cooperative effort of members from the Michigan State Police, local Michigan Police Departments, and the Federal Government, whose purpose is to investigate criminal violations of both federal and state child pornography and child exploitation laws. Your Affiant has been trained in the investigation of computer related child exploitation and child pornography cases.
2. This affidavit is based upon information I have gained from my investigation, my training and experience, and from information provided by law enforcement officers and others who have personal knowledge of the events and circumstances described herein.
3. This investigation of peer-to-peer file sharing networks is a cooperative effort of law enforcement agencies around the country. Many of these agencies are associated with the Internet Crimes Against Children (ICAC) Task Force Program. Many of the Officers/Agents involved in this effort are using the technology and methods described herein. This methodology has led to the issuance and execution of search warrants around the country resulting in the seizure of child pornography and arrests for possession and distribution of child pornography.

4. This affidavit has attached hereto and incorporated herein by reference Exhibit 1 which includes a seven page document that details peer-to-peer file sharing networks, peer-to-peer client software programs, and the eDonkey2000 (eD2K) and Kademlia (Kad) peer-to-peer file sharing networks.

5. The information set forth in this affidavit is for the limited purpose of establishing probable cause; this affidavit, therefore, does not include all the information collected during this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence of a violation of Title 18, United States Code, Sections 2252A(a)(2) and (a)(5)(B), to-wit: knowingly distributing, receiving, and possessing any visual depiction involving minors engaging in sexually explicit conduct.

DETAILS OF INVESTIGATION

6. This case originated on 6/6/12 when Affiant was conducting investigations into the use of peer-to-peer ("P2P") file sharing programs for the possession and distribution of child pornographic images and movies. While conducting this investigation, Affiant was connected to the eDonkey2000 (hereinafter referred as "eD2k") and the Kademlia (hereinafter referred as "Kad") networks, (both public file sharing networks which use the Internet) using an eD2k/Kad client software program installed on my computer. The eD2k/Kad client software program Affiant used had a unique user hash identifying my client software on the network.

7. Continuing on 6/6/12, Affiant was connected to the eD2k and Kad networks through the Internet using an eD2K/Kad P2P client program. Affiant began the

investigation by conducting searches for digital files on the eD2k network Affiant believed to contain images and/or videos of child pornography. At approximately 1720 hrs, Affiant observed a computer that recently reported that it shared at least one image file that Affiant had seen before in previous investigations and believed to contain child pornography. Affiant observed this host computer to have an Internet Protocol (IP) address of 96.27.80.22. Based on geographic mapping of this host IP address, Affiant believed the associated computer to be located in Michigan.

8. Still on 6/6/12, Affiant attempted to download the digital video file believed to contain child pornography from the remote host computer located at IP Address 96.27.80.22. Affiant was able to connect directly to the remote host computer, located at IP Address 96.27.80.22, and download the digital file. The file name was "14y Kimmy, St-Petersburg, i06-a (1).avi". The remote client's software program was eMule v0.50a with a user hash of C8558648A00E3227811F740D3CD26F2E.

9. After downloading the video file, Affiant watched it. The video depicted a female child, approximately 11 years of age, fondling/masturbating the penis of a male.

10. On 6/7/12, Affiant again observed a computer with IP address 96.27.80.22 that recently reported sharing at least one image file, which depicted child pornography, seen in previous investigations and believed to contain child pornography. At that time, Affiant attempted to download the digital video file, believed to contain child pornography, from the remote host computer located at IP Address 96.27.80.22. Affiant was able to connect directly to the remote host

computer located at IP Address 96.27.80.22 and download the digital file. The file name was "12y Daughter & 13Y Best Friend.mpg". The remote client's software program was eMule v0.50a with a user hash of C8558648A00E3227811F740D3CD26F2E.

11. After downloading the video file, Affiant viewed it. The video depicted a female child, approximately 9-11 years of age, wearing black stockings. The female child is initially fondling herself. An adult male later begins rubbing his penis on the vagina of the female child. The female child subsequently begins performing oral sex on the adult male while holding a teddy bear.

12. Based on Affiant's training and experience, the two videos, described in paragraphs nine and eleven, meet the definition of child pornography in Title 18, United States Code, Section 2256.

13. Affiant next conducted an Internet search on the origin of the IP address 96.27.80.22 and determined it was issued to the Internet service provider, Wide Open West (WOW). Affiant obtained a Grand Jury subpoena from the Eastern District of Michigan to obtain records and other information pertaining to the respective subscriber of 96.27.80.22 on 6/6/12 at 21:20:11 hrs (EDT) and 6/7/12 at 01:36:54 (EDT) hrs (EDT) from WOW.

14. It should be noted that between 6/6/12 and 6/26/12, Affiant observed approximately 40 suspected digital image/video files of child pornography available for download from the remote host computer located at IP Address 96.27.80.22.

15. On 6/27/12, WOW responded and indicated that the subscriber of IP address 96.27.80.22 on 6/6/12 and 6/7/12 was Thomas Creely, xxx Ridgemont Avenue, Dearborn, Michigan.

16. On 7/10/12, Agents from the Detroit Field Office and Michigan ICAC Task Force executed a federal search warrant at the Dearborn, Michigan, residence. Thomas and Matthew Creely were at the residence when the search warrant was executed. Pursuant to the search warrant, agents seized one Antec desktop computer tower, one cannon digital camera, and one flash drive.

17. Special Agent Kevin Nowakowski and Detective Sergeant (Det/Sgt) William Liczbinski, of the Wayne County Sherriff's Office (WCSO), interviewed Thomas Creely. During that interview, Thomas Creely indicated that WOW provided Internet service to the residence and that the home used wireless Internet access. Thomas Creely went on to say that the wireless network was set up by his son Matthew. Thomas Creely indicated that he had never seen, downloaded, or distributed any sexually explicit images/videos of minors.

18. Continuing on 7/10/12, Detective Corporal (Det/Cpl) James Isaacs, with the Dearborn Police Department (DPD), and Affiant interviewed Matthew Creely. During that interview, Matthew Creely made the following statements:

    a. He had been using bit torrent and eMule on the Antec computer to download sexually explicit images/videos of minors for approximately one year;

    b. His Antec computer tower contained approximately 1,000 digital image/video files of child pornography;

c. Most of his digital image/video files were of females between the ages of 8-13 and that they did not contained depictions of bondage or rape;

d. He knew that his eMule program was sharing his digital images/videos of child pornography with other eMule users;

e. He only used the digital image/video files that he obtained for masturbation and never showed them to anybody else, never chatted on-line with any minors, and never chatted on-line about his downloaded child pornography;

f. He used the search terms 13, pxxxe bxxxs, R@xxxxd, PxxC, nxxxot and pxxxxil when he searched for child pornographic image/video files; and

g. He had never had sexual contact with minors and never participated in any chat forums concerning pedophilia or how to obtain/trade CP on-line.

19. As of 9/7/12, Det/Sgt Liczbinski is still currently conducting the computer forensic examination of the items seized during the search warrant of the Dearborn, Michigan, residence. Det/Sgt Liczbinski stated that, although the forensic examination is not complete, at this point, he has recovered at least 1,000 digital image/video files of minors engaged in sexually explicit conduct from the Antec computer tower.

CONCLUSION

20. Based upon the information contained in this affidavit, your Affiant submits that there is probable cause to believe that Matthew T. Creely, while using any facility or means of interstate or foreign commerce, the Internet, did knowingly distribute, receive, and possess visual depictions involving real children engaged in sexually explicit conduct, in violation of Title 18, United States Code § 2252A (a)(2) and (a)(5)(B).

Special Agent Eric S. Clark
United States Secret Service

Subscribed and sworn before me this 12th day of September 2012.

DAVID R. GRAND
UNITED STATES MAGISTRATE JUDGE

Peer to Peer File Sharing

Based on my training and experience, I know the following regarding Peer to Peer file sharing networks, Peer to Peer client software programs, and the eDonkey2000 (eD2K) and Kademlia (Kad) Peer to Peer file sharing networks.

A growing phenomenon on the Internet is peer to peer (hereinafter referred to as "P2P") file sharing. P2P file sharing is a method of communication available to Internet users through the use of special software programs. P2P file sharing programs allow groups of computers using the same file sharing network and protocols to transfer digital files from one computer system to another while connected to a network, usually on the Internet. There are multiple types of P2P file sharing networks on the Internet. To connect to a particular P2P file sharing network, a user first obtains a P2P client software program for a particular P2P file sharing network, which can be downloaded from the Internet. A particular P2P file sharing network may have many different P2P client software programs that allow access to that particular P2P file sharing network or multiple P2P file sharing networks. These P2P client software programs share common protocols for network access and file sharing. The user interface, features, and configurations may vary between clients and versions of the same client.

In general, P2P client software allows the user to set up file(s) on a computer to be shared on a P2P file sharing network with other users running compatible P2P client software. A user can also obtain files by opening the P2P client software on the user's computer and conducting a search for files that are of interest and currently being shared on a P2P file sharing network.

Some P2P file sharing networks are designed to allow users to download files and frequently provide enhanced capabilities to reward the sharing of files by providing reduced wait periods, higher user ratings, or other benefits. In some instances, users are not allowed to download files if they are not sharing files. Typically, settings within these programs control sharing thresholds.

Typically, during a default installation of a P2P client software program, settings are established which configure the host computer to share files. Depending upon the P2P client

software used, a user may have the ability to reconfigure some of those settings during installation or after the installation has been completed.

Typically, a setting establishes the location of one or more directories or folders whose contents (digital files) are made available for distribution to other P2P clients. Typically, individual files can also be shared.

Typically, a setting controls whether or not files are made available for distribution to other P2P clients.

Typically, a setting controls whether or not users will be able to share portions of a file while they are in the process of downloading the entire file. This feature increases the efficiency of the network by putting more copies of file segments on the network for distribution.

Files being shared by P2P clients are processed by the client software. As part of this processing, a hashed algorithm value is computed for each file being shared, which uniquely identifies it on the network. A file processed by this hash algorithm operation results in the creation of an associated hash value often referred to as a digital signature. Some hash algorithms provide a certainty exceeding 99.99 percent that two or more files with the same hash value are identical copies of the same file regardless of their file names. By using a hash algorithm to uniquely identify files on a P2P network, it improves the network efficiency. Because of this, typically, users may receive a selected file from numerous sources by accepting segments of the same file from multiple clients and then reassembling the complete file on the local computer. This is referred to as multiple source downloads. The client program succeeds in reassembling the file from different sources only if all the segments came from exact copies of the same file. P2P file sharing networks use hash values to ensure exact copies of the same file are used during this process.

P2P file sharing networks, including the eDonkey2000 (hereinafter referred to as "eD2K") network and Kademlia (hereinafter referred to as "Kad") network, are frequently used to trade digital files of child pornography. These files include both image and movie files.

A commonly used P2P client software program is eMule. eMule is a free Microsoft Windows P2P client software program for the eD2k and Kad file sharing networks. A couple of distinguishing features of eMule are the direct exchange of sources between clients and the use of a credit system to reward frequent uploaders.

Another commonly used P2P client program is Shareaza. Shareaza is also a free Microsoft Windows P2P client, which supports multiple P2P file sharing networks, such as Gnutella, BitTorrent, and eD2k. Other computer operating system platforms, such as MacIntosh or Linux, also have P2P client software programs that access and share files on the eD2K network, such as aMule, which is similar to eMule.

The eD2k file sharing network is composed of clients and servers, the latter commonly referred to as eDonkey or eD2k servers. eMule is a publically available open source client software program, released under the GNU Public License[1]. In contrast to eMule, the most common eD2k server is a free software program, but the server source code is not freely available.

Typically, when a user launches the eMule client program, the client program will likely connect to an eD2K network server. Once connected to an eD2k server, information about the files the user is sharing is provided to that server. Such information may include the file's eD2k hash value, the file's size, and parsed keyword terms from the file name. The eD2k network uses the MD4[2] (Message Digest version 4) hash algorithm to uniquely identify files on the network.

The eD2K network servers assist the eMule client users in locating files based on the keyword terms searched for by the user. When a user wants to find a file on the eD2k network, the user enters a keyword search into the eMule search screen menu. This initiates a keyword search request to the client's eD2k server, and to other eD2k servers the client is aware of. Each server returns a list of files (not the files themselves) that match the search criteria. This information comes from clients that have recently reported that it had all or part of that file to the eD2k servers. Each file name returned is mapped to an eD2k MD4 hash value, which uniquely

[1] GNU General Public License is intended to guarantee the freedom to share and change software for all its users. General Public Licenses are designed to make sure that you have the freedom to distribute copies of the software, that you can receive the source code if you want it, and that you can change the software or use pieces of it in new programs.

[2] MD4 or Message Digest Algorithm Version 4 is a file encryption method which may be used to produce a unique digital signature of a file. The eD2k network file hash is a hash of hashes. Each 9.5MB (9728000 byte) portion of the file is computed with an MD4 hash value. An MD4 hash of those hashes is then computed to uniquely identify the file. If the file is less than 9.5MB, then the MD4 hash of the file is equivalent to the eD2k hash. The file size is also used along with the file size to identify files being shared. It is computationally infeasible to find two different files having the same eD2K MD4 hash value and size.

identifies the file on the eD2k network. In order for the user to obtain the actual file, the user must manually initiate a download process, typically by double clicking on the file name. The user can identify the file(s) they wish download by the file name and/or the file type (i.e. videos, music, images, etc…). When the download process of the file actually begins, the download of the file occurs between two or more clients (not the server[s]).

Once a user chooses to download a particular file, the eMule client will again query the eD2k servers, though this query is not visible to the user. During this query, the eMule client will essentially ask for the IP addresses[3] of other active clients that either possess this file in whole or in part. The eMule client can then use the IP addresses to directly connect to another client and request the file. Typically, once the eMule client has downloaded part of a file, it may immediately begin sharing the file with other users.

In addition to the eD2k network servers, eMule clients can use the Kad network protocols to locate files. Kad differs in that all communication is between clients, rather than relying on servers. In general the use of a Kad network versus an eD2k network server is transparent to the user. Typically the Kad network and eD2K network operate in parallel to each other and assist with making the P2P file sharing more efficient.

Typically, as described above, one method for an investigator to search the eD2K network for users possessing and/or disseminating child pornography files is to type in search terms, based on their training and experience, that would return file name results indicative of child pornography. The investigator would then download the file and determine if it indeed contained child pornography. If so, the investigator can document the eD2k MD4 hash value of this file, to be compared with future identical files observed on the eD2k network. Although transparent to the typical user, when searches are conducted, additional results are received from the eD2k servers or other clients, which may include the eD2K MD4 hash value of the file, the file size, and the IP addresses of clients who recently reported to the network as having that file in whole or in part. This information can be documented by investigators and compared to those eD2k MD4 hash values the

[3] Computers on the Internet identify each other by an Internet Protocol or IP address. IP addresses can assist law enforcement in finding a particular computer on the Internet. IP addresses can typically lead the law enforcement officer to a particular Internet service company and that company can typically identify the account that used the IP address to access the Internet.

investigator has obtained in the past and believes to be child pornography. This allows for the detection and investigation of computers involved in possessing, receiving, and/or distributing files of previously identified child pornography. Therefore, without even downloading the file, the investigator can compare the eD2K MD4 hash value and determine with mathematical certainty that a file seen on the network is an identical copy of a child pornography file they had seen before. Additionally, another investigative method allows investigators the ability, while adhering to the eD2k network protocols, to search for files they believe to be child pornography, if they know the files eD2k MD4 hash value and file size. During this type of search, the investigator can query eD2k network servers for client users who have recently reported to eD2k network servers that they have a file, in whole or in part, that matches a known eD2k MD4 hash value of a file an investigator believes to be child pornography. The eD2k network servers will respond with matching results, which include the clients' IP address(es). This is based on the eD2k MD4 hash value, as recently reported by the client to the eD2k network servers, regardless of the file name associated with that file. The returned list of IP addresses can include computers that are likely to be within the investigator's jurisdiction. The ability to identify the approximate location of these IP addresses is provided by IP geographic mapping services, which are publicly available and also used for marketing and fraud detection. At this point in the investigative process, an association between a known file (based upon on the eD2K MD4 hash value comparison) and a computer having a specific IP address (likely to be located within a specific region) can be established.

Once a client user is identified as recently having a file believed to be child pornography, in whole or in part, the investigator can then query that client user directly to confirm the client user has that file, in whole or in part, and/or download that file directly from the client user exclusively, otherwise known as a single source download. Depending upon several factors, including configuration and available resources, it might not be possible to do either. The process of sharing files on the eD2K and Kad networks involve clients allowing other clients to copy a file or portions of a file. This sharing process does not remove the file from the computer sharing the file. This process places a copy of the file on the computer which downloaded it.

If an investigator either received an affirmative response from a remote client that they possess a digital file, or the investigator received a digital file, in whole or in part, that is believed to contain child pornography, from a remote client at a specific IP address, the investigator can conclude that a computer, likely to be in this jurisdiction, is running an eD2K P2P client and is currently possessing, receiving, and/or distributing specific and known visual depictions of child pornography.

During the query and/or downloading process from a remote client, certain information is exchanged between the investigator's client and the remote client they are querying and/or downloading a file from. Such as 1) the remote client's IP address; 2) if the remote client has the file in whole or only in part; 3) the file name on the remote client's computer; 4) the eD2k MD4 hash value of the file; 5) the remote client's user hash[4]; 6) the remote client's software and version; 7) and the investigator's user hash. This information may remain on the remote client's computer system for long periods of time. The investigator has the ability to log this information. A search can later be conducted on a seized computer system(s) for this information, which may provide further evidence that the investigator's client communicated with the remote client.

An analogy to this investigative methodology would be receiving information from an informant or an anonymous source that a particular residence was selling illegal narcotics. An undercover investigator could independently confirm this information by knocking on the door of the residence and asking if they had said illegal narcotics. If so, the undercover investigator would then ask for and receive the said illegal narcotics without actually entering the residence, which would be similar to asking for and receiving an illegal child pornography file from a P2P client.

The investigation of peer-to-peer file sharing networks is a cooperative effort of law enforcement agencies around the country. Many of these agencies are associated with the Internet Crimes against Children Task Force Program. P2P investigative methodology has led to the issuance and execution of search warrants around the country resulting in the arrest and

[4] Each client generates a 16-byte identifier to uniquely identify itself, referred to as the user hash. This unique value could be compared to a serial number. It is used on this file sharing network to identify itself with other clients to receive credit for sharing files with users on this network.

conviction of numerous offenders possessing and/or distributing child pornography, some of which were also involved the sexual exploitation of actual child victims.